B.TECH.
(SEM VI) THEORY EXAMINATION 2023-24
COMPUTER NETWORKS

SECTION A

Ques 1.

Ques a. What are the applications of Computer Networks?

Ans: Applications of Computer Networks

- Exchange of information by means of e-Mails and FTP.
- Information sharing by using Web or Internet.
- Interaction with other users using dynamic web pages.
- Resource sharing such as printers and storage devices.

Ques b. Write advantages and disadvantages of Mesh Topology.

Ans: Mesh Topology Pros and Cons:

Pros	**Cons**
Data transmission is reliable	Significant duplicate connection risk
Straightforward Scalability	The strain on each node has increased
Addition of new hardware has no impact on data transmission	Latency problems

Ques c. Define fixed and variable size framing.

Ans: 1. Fixed-size: The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.
2. Variable size: In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish.

Ques d. Explain the working of Bridge.

Ans: Bridges connect and enable communication between two different networks at the data link layer in an OSI model. Bridges can also extend a network's physical size. Bridges can also be used to connect a LAN segment in one location to another LAN segment in another location via a synchronous modem connection.

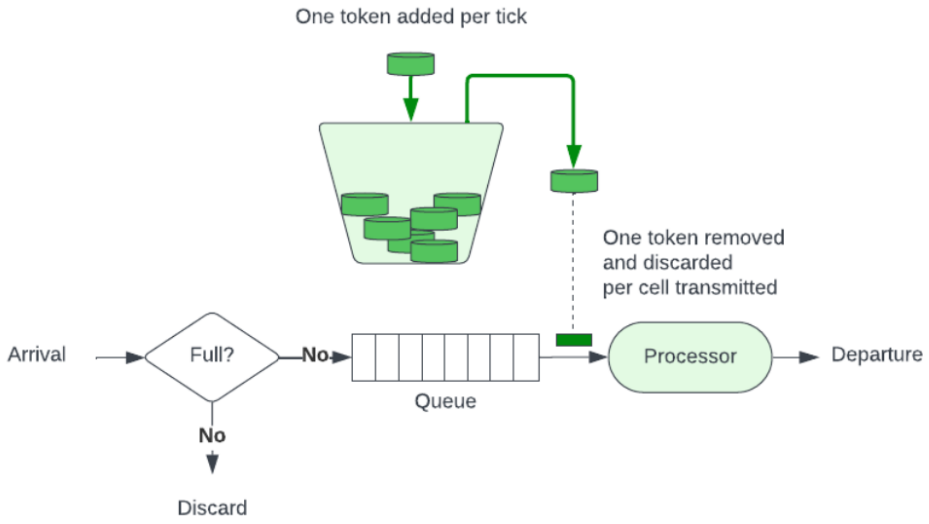
Ques e. Define delivery in Network Layer.

Ans: Network Layer is the third layer of the OSI Model. It's responsible for source-to-destination or host-to-host delivery of packets across multiple networks. This layer takes the data from the transport layer, adds its header, and forwards it to the data link layer. Delivery networking describes a system of computers networked together across the Internet that cooperate transparently to deliver content

Ques f. Define Token Bucket.

Ans: The Token Bucket algorithm is a popular and simple method used in computer networking and telecommunications for traffic shaping and rate limiting. It is designed to control the amount of data that a system can send or receive in some sort of period, ensuring that the traffic conforms to a specified rate.

It refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions, or traffic aggregates. It is something that data flow seeks to attain.



Ques g. Write about Registered ports.

Ans: Port is a logical address of a 16-bit unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.

Registered Port

- It is from range 1024 to 49151
- These are used by applications or services that are not as common
- But it is used by those applications or services that require its specific port
- Organizations can ask IANA(Internet Assigned Number Authority) for any specific port number within this range

Ques h. Differentiate between connection-less and connection-oriented.

Ans:

Connection-oriented Service	**Connection-less Service**
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)

Ques i. What is Telnet?

Ans: Telnet is a network protocol used to virtually access a computer and provide a two-way, collaborative, and text-based communication channel between two machines.

Ques j. Define Compression.

Ans: Data compression is the process of encoding, restructuring or otherwise modifying data to reduce its size. Fundamentally, it involves re-encoding information using fewer bits than the original representation.

Compression is done by a program that uses functions or an algorithm to effectively discover how to reduce the size of the data. For example, an algorithm might represent a string of bits with a smaller string of bits by using a 'reference dictionary' for conversion between them. Another example involves a formula that inserts a reference or pointer to a string of data that the program has already seen. A good example of this often occurs with image compression. When a sequence of colors, like 'blue, red, red, blue' is found throughout the image, the formula can turn this data string into a single bit, while still maintaining the underlying information.

SECTION B

Ques 2.

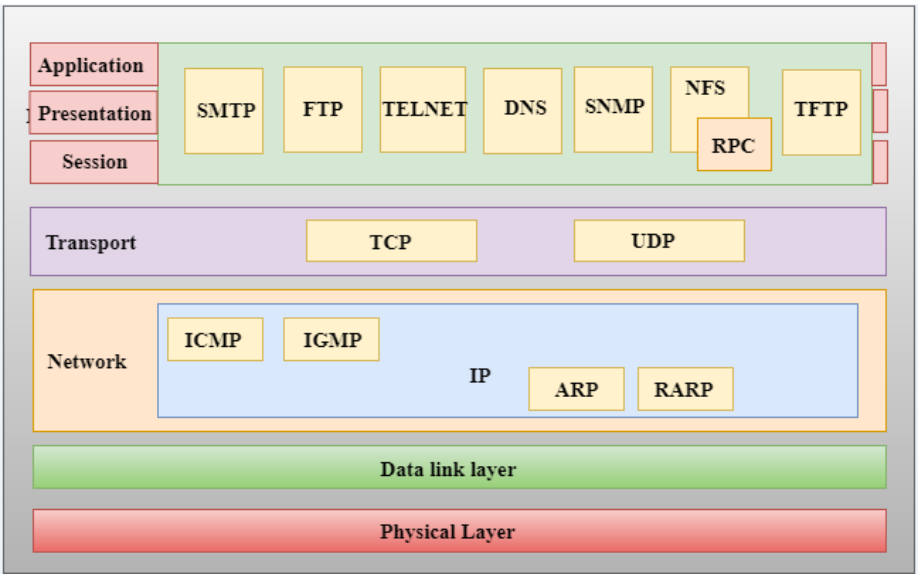
Ques a. Define TCP/IP Model in detail.

Ans: TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
- **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

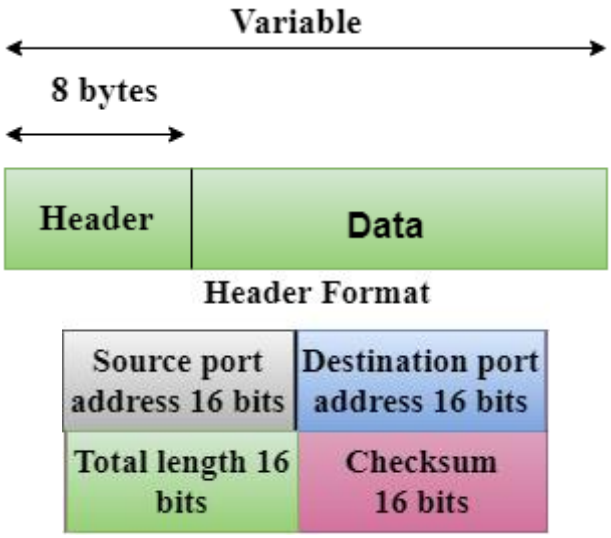
Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
    - It provides connectionless service and end-to-end delivery of transmission.
    - It is an unreliable protocol as it discovers the errors but not specify the error.
    - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
    - **UDP consists of the following fields:**
      Source port address: The source port address is the address of the application program that has created the message.
      Destination port address: The destination port address is the address of the application program that receives the message.
      Total length: It defines the total number of bytes of the user datagram in bytes.
      Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



- **Transmission Control Protocol (TCP)**

  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

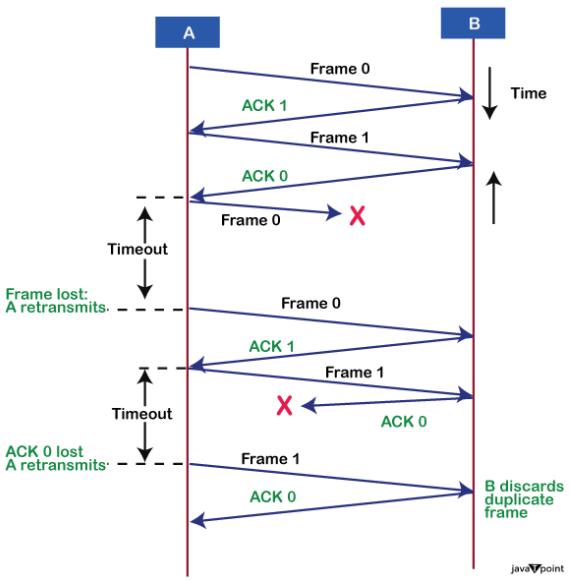
Ques b. Explain Noisy channel Protocols with explanation and diagram.

Ans: Noisy Channel Protocols encompass the Stop-and-Wait Protocol, the Sliding Window Protocol, and the Automatic Repeat Request (ARQ) Protocol.

STOP-AND-WAIT ARQ Protocol - The Stop and Wait protocol is a protocol used for dependable records transmission over a noisy channel. In this protocol, the sender simplest sends one frame at a time and waits for an acknowledgment (ACK) from the receiver earlier than sending the subsequent frame. This facilitates making certain that the receiver gets the data efficiently and gets rid of the want for retransmission within the case of mistakes as a result of the noisy channel. The sender continuously video displays the channel for mistakes, and if a blunders is detected, it waits for the next ACK before resending the body. This protocol adds blunders manipulated to the basic unidirectional communique of statistics frames and ACK frames within the opposite route.

Flow Diagram

A statistics glide diagram in the Stop-and-Wait protocol in a loud channel may be used to describe the go with the flow of information between the sender and the receiver. This diagram generally includes the following components:



Sender: The sender sends facts frames one after the other, and waits for a reaction (ACK or NACK) from the receiver before sending the following records body.

Receiver: The receiver receives the recorded frames and approaches them. If the frame is acquired efficiently, the receiver sends an ACK signal to the sender. If the body is not obtained effectively, the receiver sends a NACK sign to the sender.

Noisy Channel: The noisy channel is the medium through which the information frames are transmitted from the sender to the receiver. The channel can upload noise to the data frames, resulting in errors and corruption of the information.

Error Detection: The receiver uses errors detection strategies such as checksums to locate errors within the acquired statistics frames.

Error Correction: If a blunders is detected, the receiver sends a NACK sign to the sender, requesting a retransmission of the body.

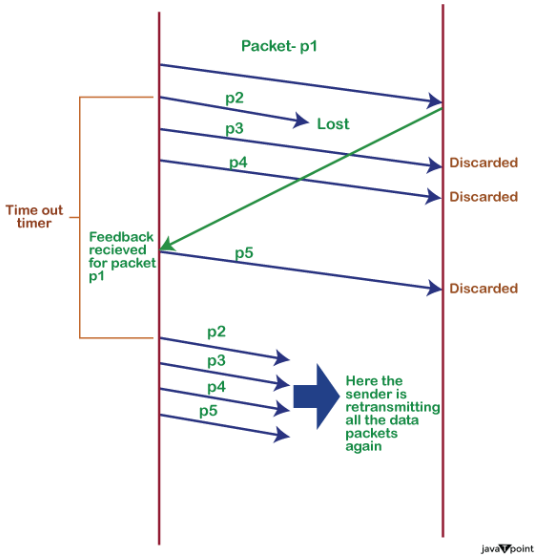
In this protocol, the sender simplest sends one data frame at a time and waits for a response from the receiver before sending the next frame. This ensures that the receiver has enough time to system each frame before receiving the subsequent one. The Stop-and-Wait protocol is reliable, however has low throughput compared to different protocols.

2. GO-BACK-N ARQ Protocol - The Go-Back-N Automatic Repeat Request (ARQ) protocol is a form of error-manipulate protocol used in data verbal exchange to ensure reliable delivery of records over a loud channel. In a noisy channel, the possibility of mistakes inside the obtained packets is excessive, and hence, there is a desire for a mechanism to hit upon and accurately identify those errors.

The Go-Back-N ARQ protocol is a kind of sliding window protocol wherein the sender transmits a window of packets to the receiver, and the receiver sends lower back an acknowledgment (ACK) to the sender indicating a receipt of the packets. In case the sender does now not receive an ACK inside a targeted timeout period, it retransmits the whole window of packets.

Flow Diagram

The waft diagram that illustrates the operation of the Go-Back-N ARQ protocol in a noisy channel:



Sender Side:

1. The sender transmits a window of packets to the receiver, starting with series range i and finishing with collection quantity i + N - 1, wherein N is the window length.
2. The sender sets a timer for each packet inside the window.
3. The sender waits for an acknowledgment (ACK) from the receiver.

Receiver Side:

1. The receiver receives the packets and exams for mistakes.
2. If a packet is acquired successfully, the receiver sends an ACK returned to the sender with the collection range of the subsequent predicted packet.
3. If a packet is obtained with errors, the receiver discards the packet and sends a poor acknowledgment (NAK) to the sender with the series variety of the following predicted packet.

Sender Side (in case of no ACK acquired):

1. If the sender does not receive an ACK earlier than the timer for a packet expires, the sender retransmits the entire window of packets beginning with the packet whose timer expired.
2. The sender resets the timer for every packet within the window.
3. The sender waits for an ACK from the receiver.

Sender Side (in case of NAK acquired):

1. If the sender receives a NAK from the receiver, the sender retransmits the packets that have not been effectively received through the receiver.
2. The sender resets the timer for each packet that was retransmitted.
3. The sender waits for an ACK from the receiver.

The above steps are repeated till all packets have been correctly obtained with the aid of the receiver. The Go-Back-N ARQ protocol provides a dependable mechanism for transmitting information over a noisy channel whilst minimizing the number of retransmissions required.

The above steps are repeated till all packets have been correctly obtained with the aid of the receiver. The Go-Back-N ARQ protocol provides a dependable mechanism for transmitting information over a noisy channel whilst minimizing the number of retransmissions required.

3. SELECTIVE REPEAT ARQ Protocol - The Selective Repeat ARQ protocol is a sort of mistakes-manipulate protocol utilized in fact communique to ensure reliable delivery of data over a noisy channel. Unlike the Go-Back-N ARQ protocol which retransmits the whole window of packets, the Selective Repeat ARQ protocol retransmits only the packets that had been now not correctly acquired.

In the Selective Repeat ARQ protocol, the sender transmits a window of packets to the receiver, and the receiver sends lower back an acknowledgment (ACK) to the sender indicating a successful receipt of the packets. If the receiver detects any blunders in a packet, it sends a bad acknowledgement (NAK) to the sender requesting retransmission of that packet.

In the Selective Repeat ARQ protocol, the sender keeps a timer for each packet within the window. If the sender does not get hold of an ACK for a packet before its timer expires, the sender retransmits handiest that packet.

At the receiver aspect, if a packet is received efficiently, the receiver sends lower back an ACK with the sequence quantity of the following anticipated packet. However, if a packet is obtained with mistakes, the receiver discards the packet and returns a NAK with the sequence variety of the packet that desires to be retransmitted.

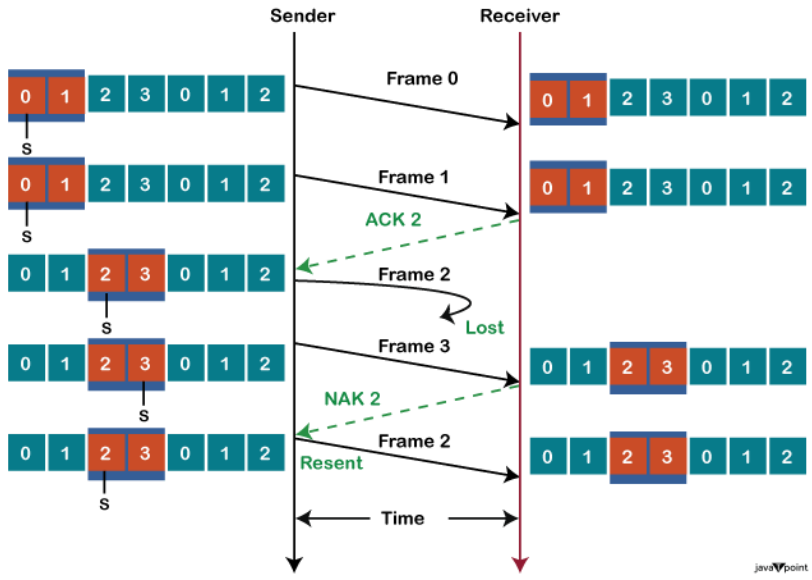
Unlike Go-Back-N ARQ, in Selective Repeat ARQ, the receiver buffer is maintained for all packets that aren't in series. When a packet with a chain quantity exclusive from the predicted collection wide variety arrives at the receiver, it's miles buffered, and the receiver sends an ACK for the final in-order packet it has received.

If a packet with a series range that the receiver has already buffered arrives, it's far discarded, and the receiver sends an ACK for the closing in-order packet it has obtained.

In summary, the Selective Repeat ARQ protocol offers a reliable mechanism for transmitting records over a loud channel whilst minimizing the quantity of retransmissions required. It retransmits simplest the packets that had been now not effectively acquired and buffers packets that arrive out of order to reduce the variety of retransmissions required.

Flow Diagram

The drift diagram that illustrates the operation of the Selective Repeat ARQ protocol in a noisy channel:



Sender Side:

1. The sender transmits a window of packets to the receiver, starting with sequence number i and ending with series wide variety i + N - 1, where N is the window length.
2. The sender sets a timer for every packet inside the window.
3. 3. The sender waits for an acknowledgment (ACK) from the receiver.

Receiver Side:

1. The receiver gets the packets and tests for mistakes.
2. If a packet is received effectively and is so as, the receiver sends an ACK lower back to the sender with the sequence quantity of the next predicted packet.
3. If a packet is received with errors or is out of order, the receiver discards the packet and sends a negative acknowledgement (NAK) to the sender with the series quantity of the packet that desires to be retransmitted.
4. The receiver buffers out-of-order packets and sends an ACK for the remaining in-order packet it has obtained.

Sender Side (in case of no ACK acquired):

1. If the sender gets a NAK from the receiver, the sender retransmits handiest of the packets that were no longer successfully received.
2. The sender resets the timer for every packet that becomes retransmitted.
3. The sender waits for an ACK from the receiver.

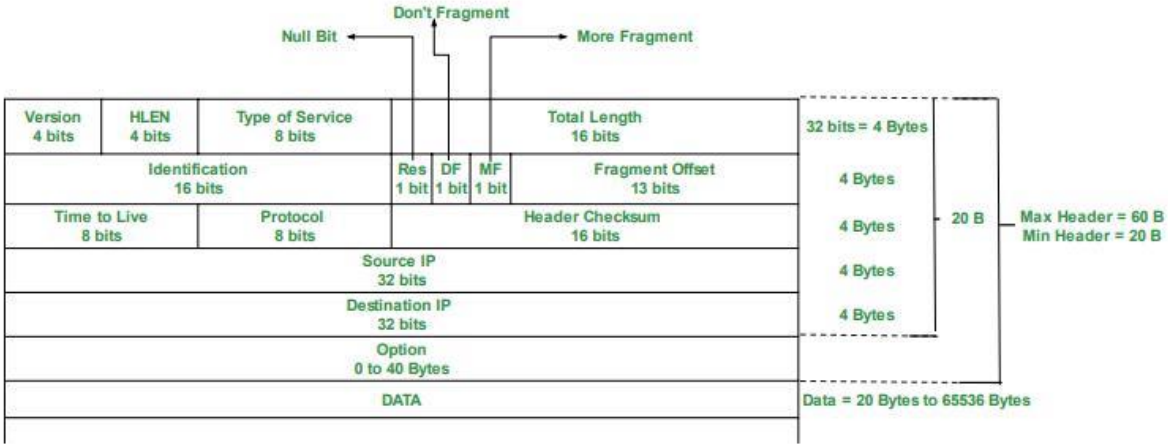
The above steps are repeated till all packets have been successfully obtained through the receiver. The Selective Repeat ARQ protocol provides a dependable mechanism for transmitting statistics over a noisy channel whilst minimizing the range of retransmissions required. It retransmits simplest the packets that have not been efficiently acquired, and buffers out-of-order packets to reduce the wide variety of retransmissions required.

Ques c. Define IPv4 header Format in detail.

Ans: IPv4 Datagram Header

- **VERSION*:*** Version of the IP protocol (4 bits), which is 4 for IPv4
- **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- **Identification*:*** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags*:*** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset:** Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- **Time to live*:*** Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum*:*** 16 bits header checksum for checking errors in the datagram header
- **Source IP address*:*** 32 bits IP address of the sender
- **Destination IP address*:*** 32 bits IP address of the receiver

- **Option:** Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.



Ques d. Define TCP features and header in detail.

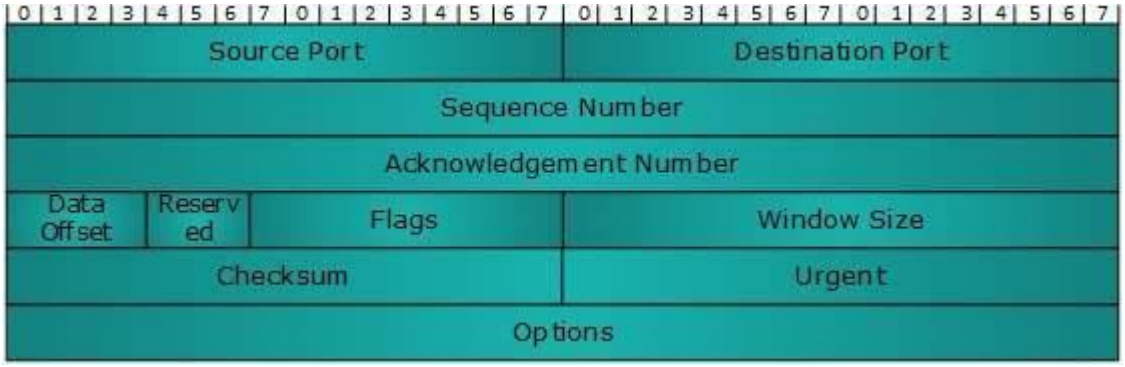
Ans: The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.

- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
    - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
    - **RST** - Reset flag has the following features:
        - It is used to refuse an incoming connection.
        - It is used to reject a segment.
        - It is used to restart a connection.
    - **SYN** - This flag is used to set up a connection between hosts.
    - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Ques e. Explain SNMP in detail.

Ans: Simple Network Management Protocol (SNMP)

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even to configure remote devices.

Components of SNMP

There are mainly three components of SNMP:

1. **SNMP Manager –** It is a centralized system used to monitor the network. It is also known as a Network Management Station (NMS). A router that runs the SNMP server program is called an agent, while a host that runs the SNMP client program is called a manager.

2. **SNMP agent –** It is a software management software module installed on a managed device. The manager accesses the values stored in the database, whereas the agent maintains the information in the database. To ascertain if the router is congested or not, for instance, a manager can examine the relevant variables that a router stores, such as the quantity of packets received and transmitted.

3. **Management Information Base –** MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables. A MIB, or collection of all the objects under management by the manager, is unique to each agent. System, interface, address translation, IP, udp, and egp , icmp, tcp are the eight categories that make up MIB. The mib object is home to these groups.

SNMP messages

- **GetRequest** : It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- **GetNextRequest :** To get the value of a variable, the manager sends the agent the GetNextRequest message. The values of the entries in a table are retrieved using this kind of communication. The manager won't be able to access the values if it doesn't know the entries' indices. The GetNextRequest message is used to define an object in certain circumstances.
- **SetRequest :** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- **Response :** When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
- **Trap :** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
- **InformRequest :** It was added to SNMPv2c and is used to determine if the manager has received the trap message or not. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

SNMP security levels

The type of security algorithm applied to SNMP packets is defined by it. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv** – This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.
2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

SECTION C

Ques 3.

Ques a. Name and explain Network Devices on each layer of OSI Model.

Ans: 1. Physical Layer (Layer 1)

- **Hub**: A basic networking device that connects multiple Ethernet devices in a local network. It operates at the bit level, broadcasting incoming data to all ports, without distinguishing between devices.
- **Repeater**: An electronic device that receives a signal and retransmits it at a higher power level to cover longer distances. It helps in extending the range of the network by amplifying the signal.

2. Data Link Layer (Layer 2)

- **Switch**: A more advanced device than a hub, it connects devices in a network and uses MAC (Media Access Control) addresses to forward data only to the specific device that needs it. This reduces unnecessary traffic and improves overall network performance.
- **Bridge**: Used to connect and manage traffic between two different LAN segments, bridges filter data based on MAC addresses, reducing collisions and improving traffic flow.

3. Network Layer (Layer 3)

- **Router**: A critical device that routes data from one network to another based on IP addresses. It determines the best path for data packets to travel across interconnected networks, using routing tables and protocols like OSPF or BGP.
- **Layer 3 Switch**: Combines the functionality of a traditional switch (operating at Layer 2) and a router. It can perform routing functions within the same network, providing faster data transfer by processing routing at the hardware level.

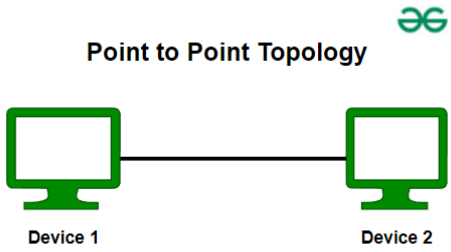
4. Transport Layer (Layer 4)

- **Gateway**: Often multifunctional, gateways connect networks using different protocols. They translate data from one protocol stack to another, enabling communication between different network architectures.
- **Firewall**: Positioned at the boundary between an internal network and an external network, firewalls filter traffic based on a set of security rules, blocking unauthorized access while allowing legitimate communication.

Ques b. Define various topologies with diagram, features, and pros-cons.

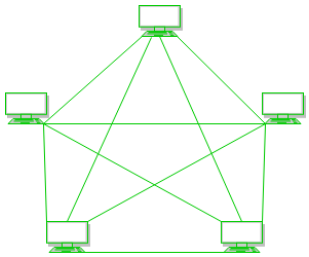
Ans: Types of Network Topology
The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

Point to Point Topology
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Mesh Topology
In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Mesh Topology

Figure 1: Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

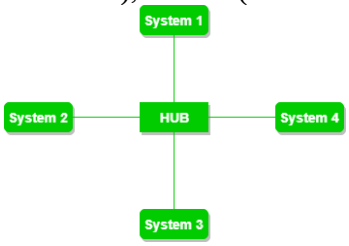
Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Star Topology

Figure 2: A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

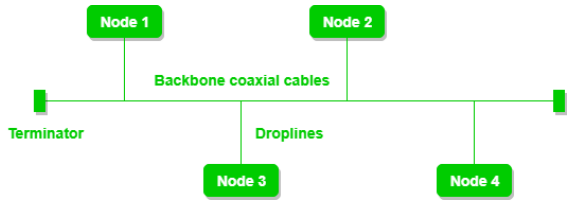
Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

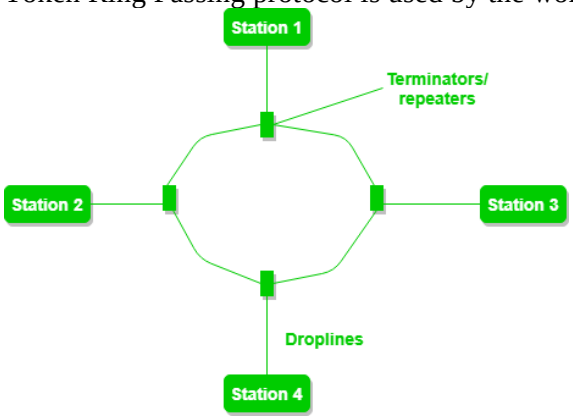
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

Figure 4: A ring topology comprises 4 stations connected with each forming a ring.

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Ques 4.

Ques a. Define any 5 LAN standards.

Ans: Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. To handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.

Types:

1. Fast Ethernet: This type of Ethernet network uses cables called twisted pair or CAT5. It can transfer data at a speed of around 100 Mbps (megabits per second). Fast Ethernet uses both fiber optic and twisted pair cables to enable communication. There are three categories of Fast Ethernet: 100BASE-TX, 100BASE-FX, and 100BASE-T4.
2. Gigabit Ethernet: This is an upgrade from Fast Ethernet and is more common nowadays. It can transfer data at a speed of 1000 Mbps or 1 Gbps (gigabit per second). Gigabit Ethernet also uses fiber optic and twisted pair cables for communication. It often uses advanced cables like CAT5e, which can transfer data at a speed of 10 Gbps.
3.10-Gigabit Ethernet: This is an advanced and high-speed network that can transmit data at a speed of 10 gigabits per second. It uses special cables like CAT6a or CAT7 twisted-pair cables and fiber optic cables. With the help of fiber optic cables, this network can cover longer distances, up to around 10,000 meters.
4. Switch Ethernet: This type of network involves using switches or hubs to improve network performance. Each workstation in this network has its own dedicated connection, which improves the speed and efficiency of data transfer. Switch Ethernet supports a wide range of speeds, from 10 Mbps to 10 Gbps, depending on the version of Ethernet being used.

Key Features of Ethernet

1. **Speed:** Ethernet is capable of transmitting data at high speeds, with current Ethernet standards supporting speeds of up to 100 Gbps.
2. **Flexibility:** Ethernet is a flexible technology that can be used with a wide range of devices and operating systems. It can also be easily scaled to accommodate a growing number of users and devices.
3. **Reliability:** Ethernet is a reliable technology that uses error-correction techniques to ensure that data is transmitted accurately and efficiently.
4. **Cost-effectiveness:** Ethernet is a cost-effective technology that is widely available and easy to implement. It is also relatively low-maintenance, requiring minimal ongoing support.
5. **Interoperability:** Ethernet is an interoperable technology that allows devices from different manufacturers to communicate with each other seamlessly.

Ques b. Explain all Random-Access protocols.

Ans: Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

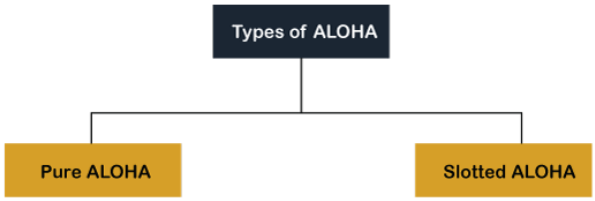
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

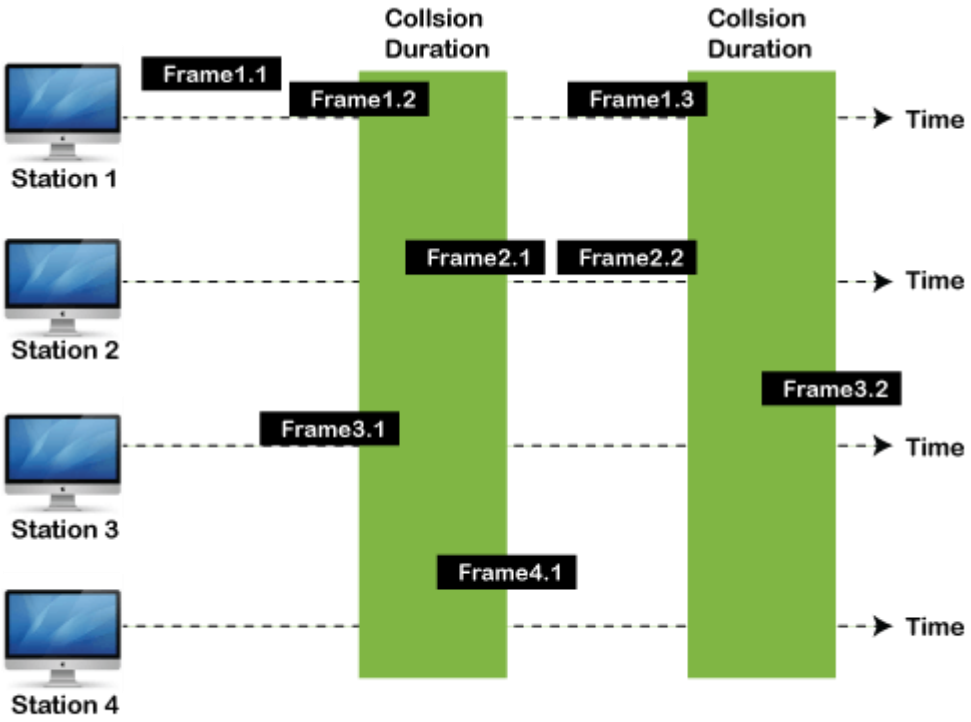
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



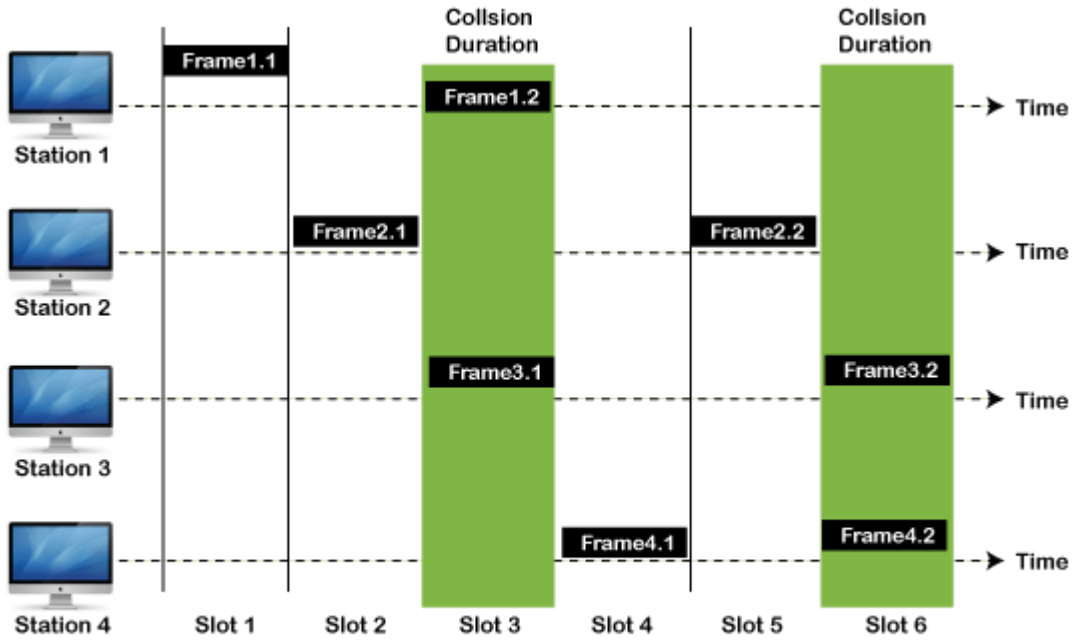
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

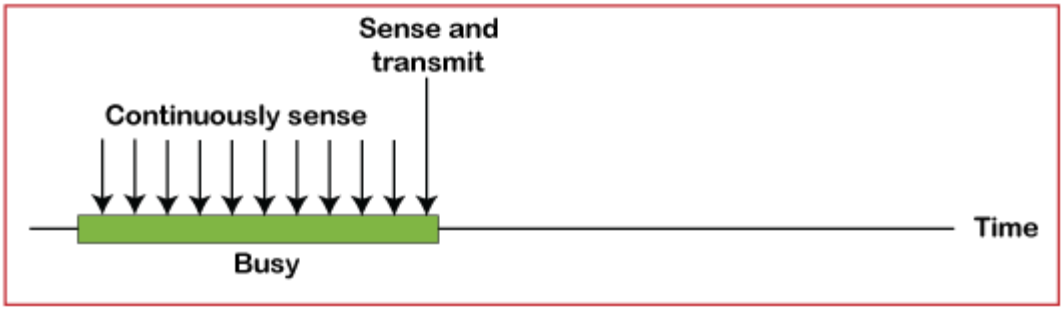
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

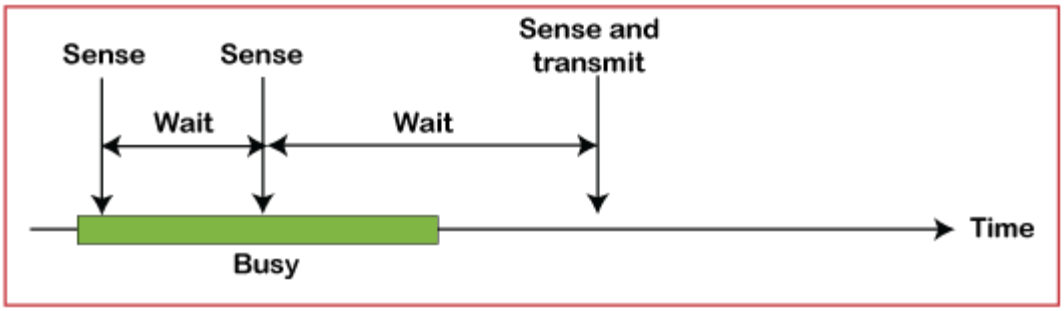
Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

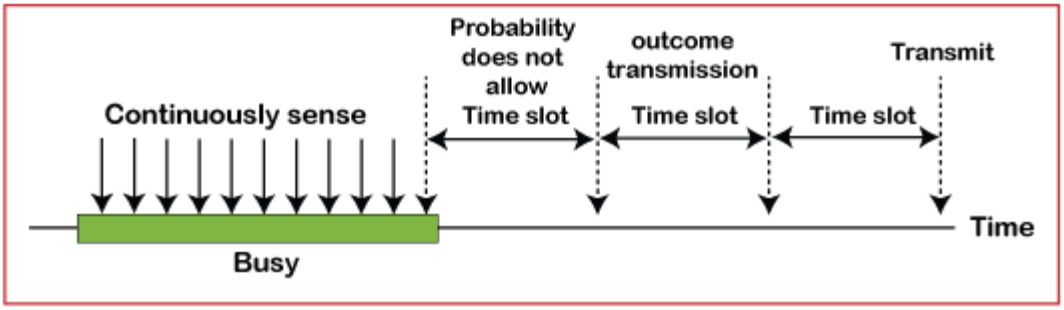
O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Ques 5.

Ques a. Explain all Interdomain and Intradomain routings algorithms.

Ans:

Key	Interdomain Routing	Intradomain Routing
Definition	Interdomain Routing, as name suggests, is the protocol in which the Routing algorithm works within and in between the domains.	Intradomain Routing is a protocol in which the Routing algorithm works only within the domains.
Information Required	In case of Interdomain routing, the interaction is across various domains, so it requires information of components of other domains.	Intradomain Routing has to interact within the domain, so it requires the information of only those components which are within the domain.
Protocols Used	In Interdomain Routing, Interior-gateway protocols such as RIP (resource information protocol) and OSPF (open shortest path first) are being used.	In Intradomain Routing, additional exterior-gateway protocols such as BGP (Border Gateway Protocol) are used.
Prerequisite	Internet connectivity should be available both within the domain and in the domain with which the interaction is taking place.	Internet connectivity should be available within the domain and during the transmission.
Complex and Dependent	Interdomain Routing is more complex and more dependent as compared to Intradomain Routing.	Intradomain Routing is less complex and less interdependent than Interdomain Routing.

Border Gateway Protocol (BGP)

- **Purpose**: BGP is designed to manage how packets are routed across the internet through the exchange of routing and reachability information between different autonomous systems.
- **Characteristics**:
  - **Path Vector Protocol**: BGP maintains the path information that gets updated dynamically.
  - **Policy-Based Routing**: BGP can enforce routing policies based on various criteria such as the shortest path, path stability, or economic considerations.
  - **Scalability**: BGP is scalable to handle the vast number of routes required on the global internet.
- **Operations**:
  - **Neighbor Establishment**: BGP peers (routers) establish a TCP connection to exchange routing information.
  - **Route** : BGP routers advertise the best paths to reach different networks.
  - **Route Selection**: BGP uses attributes like AS-path, next-hop, and local preference to select the best route.

Intradomain Routing Algorithms

Intradomain routing, also known as interior gateway routing, occurs within a single autonomous system. Common protocols include OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and IS-IS (Intermediate System to Intermediate System).

Open Shortest Path First (OSPF)

- **Purpose**: OSPF is used for routing within an AS, ensuring efficient and loop-free routing.

- **Characteristics**:
  - **Link-State Protocol**: Each router maintains a map of the network and uses Dijkstra's algorithm to compute the shortest path.
  - **Hierarchical Design**: OSPF supports a two-level hierarchy with areas to optimize traffic and reduce overhead.
  - **Fast Convergence**: OSPF quickly adapts to network changes.
- **Operations**:
  - **Hello Protocol**: Used to establish and maintain neighbor relationships.
  - **Link-State s (LSAs)**: Routers exchange LSAs to build a complete network topology.
  - **Shortest Path First Calculation**: Each router independently calculates the best paths using the Dijkstra algorithm.

Routing Information Protocol (RIP)

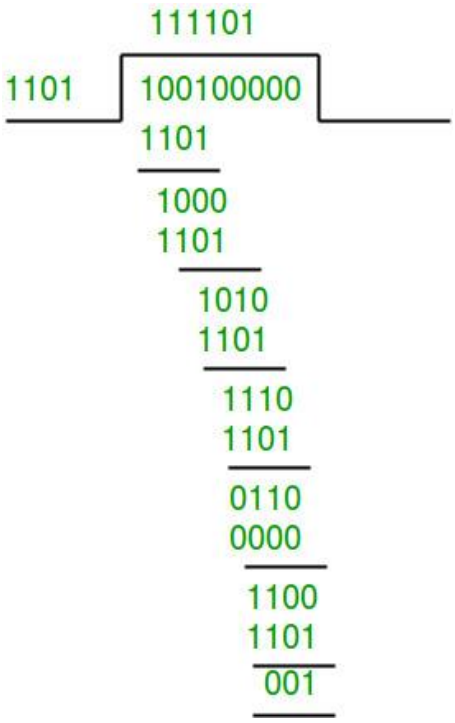
- **Purpose**: RIP is a simple distance-vector protocol used in smaller networks.
- **Characteristics**:
  - **Distance-Vector Protocol**: Uses hop count as the metric, with a maximum hop count of 15.
  - **Periodic Updates**: Routers send their routing tables to neighbors every 30 seconds.
  - **Simple Configuration**: Easy to configure but less efficient for large or complex networks.
- **Operations**:
  - **Routing Updates**: Routers broadcast their entire routing table periodically.
  - **Route Calculation**: Routes are determined based on the hop count to the destination.

Ques b. Senders' data D= 110101, CRC generator polynomial=x3+x+1. Apply CRC algorithm and Perform calculations both at sender and receiver end.

Ans: Data word to be sent - 100100

Key - 1101 [Or generator polynomial x3 + x2 + 1]

Sender Side:



Therefore, the remainder is 001 and hence the encoded data sent is 100100001.

Receiver Side:
Code word received at the receiver side 100100001

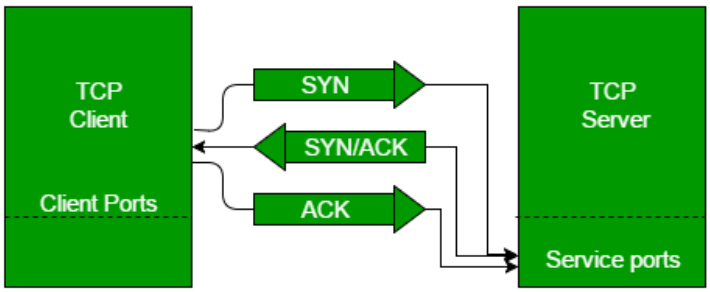
```
          111101
       ┌─────────
1101   │100100001
       │ 1101
       │ ----
       │  1000
       │  1101
       │  ----
       │   1010
       │   1101
       │   ----
       │    1110
       │    1101
       │    ----
       │     0110
       │     0000
       │     ----
       │      1101
       │      1101
       │      ----
       │      0000
       │      ----
```

Therefore, the remainder is all zeros. Hence, the data received has no error.

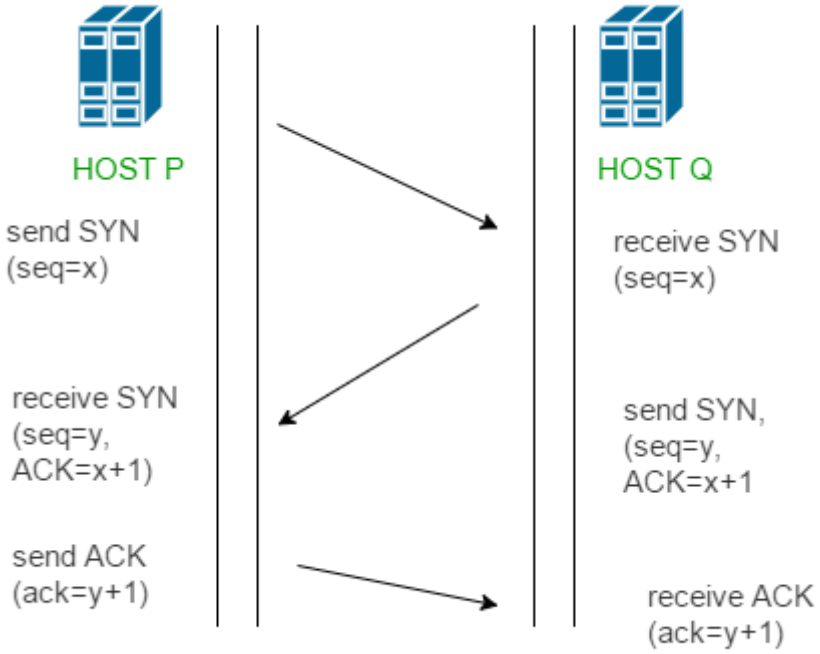
Ques 6.

Ques a. Define Connection Management. Explain how Three-way handshaking using diagram.

Ans: Connection management in networking refers to the process of establishing, maintaining, and terminating connections between devices or systems within a network.
The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model). The Application layer is a top pile of a stack of TCP/IP models from where network referenced applications like web browsers on the client-side establish a connection with the server. From the application layer, the information is transferred to the transport layer where our topic comes into the picture. The two important protocols of this layer are – TCP, **UDP(User Datagram Protocol)** out of which TCP is prevalent(since it provides reliability for the connection established). However, you can find an application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.



TCP provides reliable communication with something called **Positive Acknowledgement with Re-transmission(PAR)**. The Protocol Data Unit(PDU) of the transport layer is called a segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), the receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from the above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. Let us delve into how this mechanism works :



- **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

Ques b. Write about Quality-of-Service Parameters.

Ans: Quality of Service (QoS) in networking refers to the overall performance of a network service, particularly the performance seen by the users of the network. Various parameters are used to measure and ensure QoS, ensuring that network traffic is managed to reduce latency, jitter, and packet loss, and to provide bandwidth guarantees. Here are key QoS parameters:

1. Bandwidth

- **Definition**: The maximum rate of data transfer across a network path.

- **Importance**: Ensures that sufficient capacity is available to handle the volume of traffic without congestion.
- **Measurement**: Typically measured in bits per second (bps).

2. Latency

- **Definition**: The time it takes for a packet to travel from the source to the destination.
- **Importance**: Critical for applications requiring real-time interaction, such as VoIP and video conferencing.
- **Measurement**: Measured in milliseconds (ms).

3. Jitter

- **Definition**: The variation in packet arrival times.
- **Importance**: High jitter can cause problems for real-time applications like VoIP and streaming media.
- **Measurement**: Measured as the variance in latency over time.

4. Packet Loss

- **Definition**: The percentage of packets that are sent but not successfully received.
- **Importance**: Can severely affect the quality of audio, video, and data transmissions.
- **Measurement**: Expressed as a percentage of lost packets out of the total sent.

5. Throughput

- **Definition**: The actual rate of successful data transfer over a network.
- **Importance**: Reflects the actual performance as experienced by the users.
- **Measurement**: Measured in bits per second (bps).

Ques 7.

Ques a. Differentiate between FTP and HTTP.

Ans:

S.NO.	HTTP	FTP
1.	It stands for HyperText Transfer Protocol.	It stands for File Transfer Protocol
2.	It is the set of rules that how web pages are transferred on different computers over the internet.	It is the set of rules that permit the downloading and uploading the files on the computer over the internet.
3.	It only supports the data connection.	It supports both data connection and control connection
4.	It uses Transmission Control Protocol and runs on TCP port 80.	It uses Transmission Control Protocol and runs on TCP port 20 and TCP port 21.

5.	The URL using the HTTP protocol will start with HTTP.	The URL using the FTP will start with FTP.
6.	It does not require authentication.	It requires authentication.
7.	It is efficient in transferring small files.	It is efficient in transferring large files.
8.	The files transferred to the computer over the internet are not saved to the memory.	The files transferred to the computer over the internet are saved to the memory.
9.	HTTP is used to provide the web pages to the web browser from the webserver	FTP is used to upload or download files between client and server.
10.	It is a stateless protocol.	It is not a stateless protocol and it maintains states.
11.	It supports an In-band type of band transfer.	It supports an Out-of-band type of band transfer.
12.	It can use both types of Persistent and Non-persistent TCP connection.	It uses a Persistent TCP connection for the Control connection and a Non-persistent TCP Connection for Data Connection.
13.	Its RFCs are 2616, 7230 and 7231.	Its RFCs are 959, 765, 1732.
14.	It uses one way communication system.	It uses two way communication system.
15.	HTTP is faster.	FTP is slower as compared to HTTP.

Ques b. Explain Cryptography. Write about RSA Algorithm with example.

Ans: Cryptography is the practice of securing information by transforming it into an unreadable format, known as ciphertext. Only authorized parties can decipher the ciphertext back into its original form, called plaintext, using decryption techniques. It plays a crucial role in protecting sensitive data in various applications, including online communication, financial transactions, and secure storage.

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests some data.

2. The server encrypts the data using the client's public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Let us learn the mechanism behind the RSA algorithm : >> Generating Public Key:

Select two prime no's. Suppose **P = 53 and Q = 59.**
Now First part of the Public key : n = P*Q = 3127.
We also need a small exponent say **e :**
But e Must be
An integer.
Not be a factor of Φ(n).
1 < e < Φ(n) [Φ(n) is discussed below],
Let us now consider it to be equal to 3.
Our Public Key is made of n and e

>> Generating Private Key:

We need to calculate Φ(n) :
Such that **Φ(n) = (P-1)(Q-1)**
so, Φ(n) = 3016
Now calculate Private Key, **d :**
d = (k*Φ(n) + 1) / e for some integer k
For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"**:

Convert letters to numbers : H = 8 and I = 9
Thus **Encrypted Data c = (89e)mod n**
Thus our Encrypted Data comes out to be 1394
Now we will decrypt **1394** :
Decrypted Data = (cd)mod n
Thus our Encrypted Data comes out to be 89
8 = H and I = 9 i.e. "HI".